Elementos de Criptografia

Curso de Licenciatura em Matemática Aplicada e Computação

Exame Tipo.
Nota mínima: 5 val

Duração: 3 horas

Grupo I 1.0(Z1); 1.0; 1.0; 1.0(Z2); 1.0; 1.0(Z3);

1. Descreva o algoritmo de encriptação do DES em pseudo-código.

2. Seja $\mathcal{E}$ um sistema criptográfico estocástico onde $\mathbf{X} = \mathbf{C}$, mostre que:
a) $H(\mathbf{q}_x|\mathbf{q}_c) = H(\mathbf{q}_c)$;
b) a ambiguidade de chave de $\mathcal{E}$ é igual a $2H(\mathbf{q}_x) - H(\mathbf{q}_y)$.

3. a) Implemente o sistema criptográfico RSA em Mathematica e mostre que a encriptação e decifração são funções inversas. Justifique a necessidade de usar primos grandes nos sistemas RSA. b) Defina em pseudo-código o teste de primalidade de Solovay-Strassen e demonstre o critério de Euler.

4. a) Defina curva elíptica sobre $\mathbb{Z}_p$ e encontre os pontos de $E(\mathbb{Z}_5)$ onde E é definida por $y^2 = x^3 + x + 1$. b) Descreva o algoritmo de assinatura do ECDSA em pseudo-código.

5. Mostre que o protocolo de troca de chaves de Diffie-Hellman pode ser atacado pelo método do *intruso-no-meio*. Indique o que é necessário adicionar ao protocolo para que este ataque não seja possível.

6. Forneça um método para um executivo distribuir uma chave de um recurso a três dos seus subordinados, de forma a que sejam necessários no mínimo dois subordinados para aceder ao recurso.

Grupo II 3,5; 2,5

1. Provas de resultados ou passos de provas de resultados realizadas nas aulas.

2. Provas de pequenos resultados não provados directamente nas aulas.